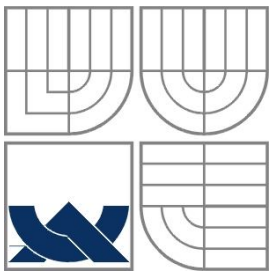
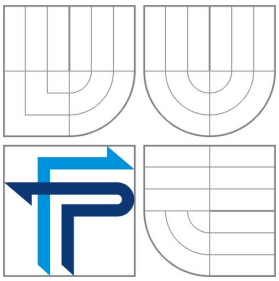


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH BEZPEČNOSTNÍ POLITIKY IS/IT VE FIRMĚ TOP MORAVIA Q, S.R.O.

IS/IT SECURITY POLICY MANAGEMENT SCHEME FOR TOP MORAVIA Q, S.R.O.

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — ONDŘEJ ŠIPKA
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2008

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2007/08
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Šipka Ondřej

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Návrh bezpečnostní politiky IS/IT ve firmě Top Moravia Q, s.r.o.

v anglickém jazyce:

IS/IT security policy management scheme for Top Moravia Q, s.r.o.

Pokyny pro vypracování:

Úvod
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN 36 9786 – ČSN ISO/IEC 13335 1-4 – Informační technologie – Směrnice pro řízení bezpečnosti IT
ČSN 36 9790 – ČSN ISO/IEC 17799 – Informační technologie – Soubor postupů pro management bezpečnosti informací
ČSN 36 9789 – ČSN ISO/IEC 15408 1-3 – Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT
DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat, Computer Press, 2004, ISBN: 80-251-0106-1
DOSEDĚL, T.: 21 základních pravidel počítačové bezpečnosti, Computer Press, 2005, ISBN: 80-251-0574-1
PROSISE, CH., MANDIA,K.: Počítačový útok Detekce, obrana a okamžitá náprava, Computer Press, 2002, ISBN 80-7226-682-9
NORTHCUTT, S. a kol.: Bezpečnost počítačových sítí, Computer Press, 2005, ISBN: 80-251-0697-7
HANÁČEK, P., STAUDEK, J.: Bezpečnost informačních systémů, ÚSIS, Praha, 2000, ISBN 80-238-5400-3

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2007/08.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. Ing. Miloš Koch, CSc.
Děkan fakulty

V Brně, dne 15.2.2008

Abstrakt

Tato práce se zabývá zhodnocením stávajícího stavu zabezpečení informačních systémů a technologií v konkrétní firmě, stanovením optimálního řešení analyzovaných bezpečnostních rizik a vytvořením bezpečnostní politiky IS.

Abstract

This thesis deals with evaluation of current security status of information systems and technologies in a given company. It determines optimal solution of analyzed security risks and creates IS security policy.

Klíčová slova

bezpečnost, bezpečnostní politika, analýza rizik, řízení bezpečnosti, směrnice IS/IT, krizové plány, zálohování dat

Keywords

security, security policy, risk analysis, safety control, IS/IT instructions, crysis plans, data backup

Bibliografická citace

ŠIPKA, O. Návrh bezpečnostní politiky IS/IT ve firmě Top Moravia Q, s.r.o.. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2008. 61 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Prohlášení autora o původnosti práce

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně, dne 28. května 2008 ……

Podpis

Poděkování

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce, panu Ing. Viktoru Ondrákovi, Ph.D. za cenné připomínky a rady poskytnuté při zpracování této bakalářské práce. Rovněž bych rád poděkoval generálnímu řediteli firmy TOP MORAVIA Q, s.r.o. panu Ing. Petru Vaněčkovi za poskytnutí všech potřebných informací.

Obsah

Úvod

Informační systémy a technologie dovolují firmám dosáhnout vyšších výkonů, a to s menším počtem zaměstnanců. Tím se snižují náklady a zvyšuje se konkurenceschopnost. Stále se vyvíjející nové a nové technologie nám usnadňují práci, na druhou stranu ale existují lidé, kteří využívají neznalostí běžných pracovníků v oblasti IS/IT ke svému vlastnímu profitu. Zvláště v době, kdy dochází ke globalizaci a většina firem využívá síť Internet, se stávají informační systémy zranitelnější proti hrozbám, které mohou omezit, či dokonce zcela zastavit chod společnosti. Každá firma by si toto nebezpečí měla uvědomit a na základě analýzy rizik eliminovat nejvážnější hrozby.

Cíl práce

Cílem této práce je navrhnout řešení, které zlepší stávající stav zabezpečení informačních systémů a dat v konkrétní firmě, vytvořit bezpečnostní politiku IS a vnitřní předpisy, určit pravomoci a odpovědnosti jednotlivých zaměstnanců při práci s počítačem.

Mnou navržené řešení sníží riziko ztráty konkrétní firmy v důsledku havárie IS, zlepší právní i fyzickou ochranu důležitých dat a určí pravomoci a odpovědnosti jednotlivých zaměstnanců.

1 Analýza současného stavu

V této kapitole popíši současný stav zabezpečení IS/IT firmy Top Moravia Q, s.r.o., a to včetně zjištěných nedostatků.

1.1 Informace o firmě

Společnost Top Moravia Q, s.r.o. vznikla v roce 2000 a v současné době zaměstnává 44 zaměstnanců. Podnik je součástí holdingu, který se zabývá výrobou vysoce kvalitního titanového nádobí a jeho přímým prodejem. Nádobí je vyráběno v kooperaci s dceřinnými společnostmi, specializovanou slévárnou hliníku a velkokapacitní lakovací linkou. Základním prodejním nástrojem podniku a jeho dceřinných společností je přímý prodej konečným zákazníkům na sálových prezentačních akcích.

Hlavní provozovna s administrativními kancelářemi a skladem se nachází v Brně, slévárna hliníku v Benešově a lakovací linka v Adamově. Roční obrat firmy Top Moravia Q, s.r.o. je přibližně 310 mil. Kč.

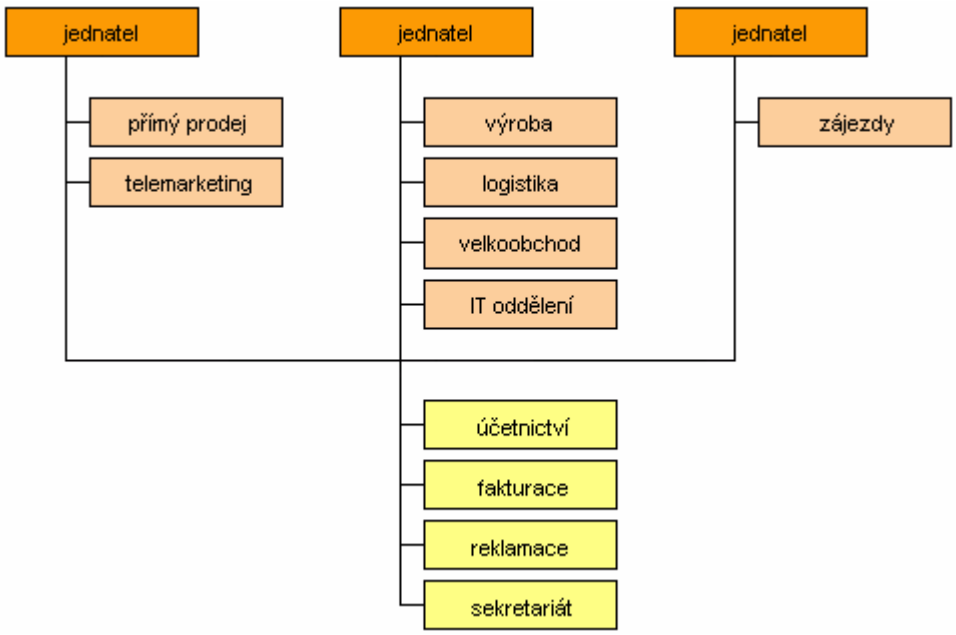
1.1.1 Organizační struktura holdingu

Výrobu v holdingu firem Top Moravia Q s.r.o. zajišťují dceřinné firmy Top Alulit s.r.o., kde se odlévají hliníkové hrnce a dále putují do provozovny firmy TPT Coating s.r.o., kde se na odlitky nanáší titanová vrstva. Následně se hrnce dovezou do skladovacích prostor firmy Top Moravia Q s.r.o., kde se instalují úchytky a poklice a balí se do krabic jako hotové výrobky. Top Moravia Q s.r.o. pak vyrobené nádobí prodává v ČR, prodej na Slovensku je zajištěn prostřednictvím dceřinné společnosti Top Slovakia Q Art, s.r.o.

Obrázek 1: Organizační struktura holdingu

1.1.2 Organizační struktura

Organizační struktura firmy je znázorněna na následujícím schématu. Firmu vlastní celkem 3 spolumajitelé (jednatelé), kteří zároveň zastávají pozice vrcholového vedení. Každý jednatel má na starosti určitá oddělení, přičemž o nejdůležitějších záležitostech se domlouvají společně.

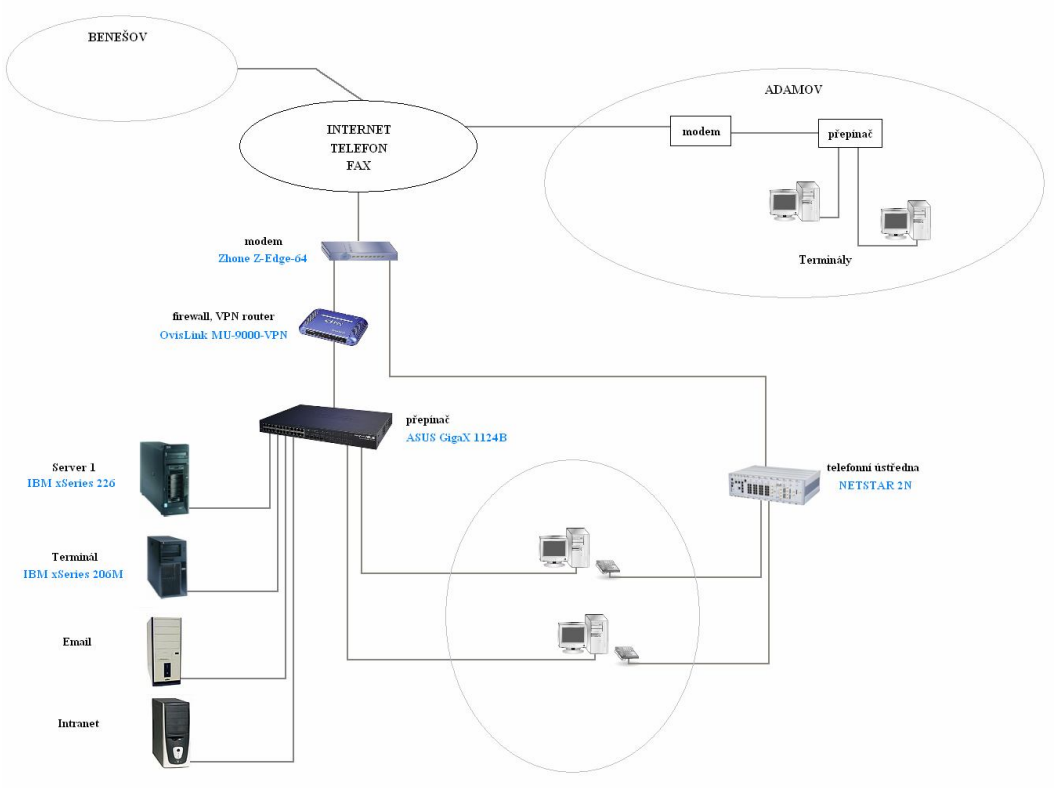


Obrázek 2: Organizační struktura

1.2 Počítačová síť

V budově je umístěno celkem 22 počítačů, 8 notebooků a 4 servery. Počítače jsou do firemní sítě připojeny hvězdicovou topologií, kdy je každý počítač pomocí vlastního kabelu připojený k centrálnímu přepínači (switchi). Celá architektura je postavena na 1Gbit/s Ethernetu. Přístup k internetu je realizován pomocí HDSL modemu a chráněn firewallem. O chod pracovních stanic se stará jeden pracovník IT, správu jednotlivých serverů zajišťují externí firmy.

Komunikace s dceřinnými firmami probíhá přes internetové připojení pomocí služby Terminal Services. Přes toto připojení se dceřinné firmy připojují na terminál umístěný v hlavní provozovně v Brně. Komunikace je zabezpečena pomocí PPTP (Point-to-Point Tunneling Protocol) tunelu. Dceřinným společnostem je poskytnut přístup do informačního systému ByznysWin, který slouží zejména pro vedení účetnictví. Někteří zaměstnanci, zejména manažeři a obchodní zástupci mají vzdálený přístup k Intranetu a e-mailům.



Obrázek 2: Architektura IT

1.2.1 Aktivní prvky

1.2.1.1 Modem

Pro připojení vnitřní počítačové sítě do telefonní sítě a na síť Internet je použit modem Zhone Z-Edge-64-BH2A. Pomocí jedné HDSL linky je realizováno jak datové připojení k síti Internet (download i upload 2 Mb/s), tak hlasové připojení do telefonní sítě (3 ISDN linky) a faxové připojení (1 linka). Modem umožňuje správu pomocí webového prohlížeče.

1.2.1.2 Switch

Všechny pracovní stanice jsou do sítě připojeny hvězdicovou topologií pomocí dvou přepínačů Asus GigaX 1124B, kdy každý disponuje 24 Gigabitovými porty. Tyto přepínače neumožňují správu, jedná se o základní přepínače pro výstavbu středně velkých sítí.

1.2.1.3 Firewall

Připojení k Internetu je chráněno firewallem OvisLink MU-9000VPN. Podle informací zaměstnanců firmy Top Moravia Q slouží zejména jako VPN (Virtual Private Network) router pro připojení dceřinných firem pomocí služby Terminal Services na terminál umístěný v hlavní provozovně v Brně. Při zjišťování nastavení tohoto firewallu vyšlo najevno, že služba VPN není na routeru zapnuta. Veškerá data mezi dceřinnými firmami a hlavní provozovnou prochází sítí Internet zabezpečena pomocí PPTP (Point-to-Point Tunneling Protocol) nakonfigurovaném na serveru TERMINAL.

Router OvisLink MU-9000VPN disponuje kromě již zmíněného VPN i FTP serverem, SPI firewallem, DHCP serverem, filtrem IP paketů, URL filtrem a přidělováním šířky pásma (QoS bandwidth management). Správa zařízení se provádí přes webové rozhraní. Ze všech funkcí, kterými tento router disponuje, je nakonfigurováno pouze přesměrování portů (port forwarding – zde pojmenováno jako Virtual Server) a spuštěn DHCP server.

Tabulka 1: Nastavení Virtual Serveru

název	protokol	port	popis
server EMAIL	tcp	25	e-mail
	tcp	22	ssh
	tcp	110	pop3
server TERMINÁL	tcp	1723	pptp
	udp	1723	pptp
	tcp	3389	rdp
server INTRANET	tcp	24	ssh
	tcp	20-21	ftp
	tcp	443	https

Nedostatky:

- Firewall neumožňuje monitorovat uživatele na Internetu
- Není určena odpovědná osoba za konfiguraci firewallu

1.2.2 Servery

Firma vlastní celkem 4 servery, z nichž 2 jsou od fy. IBM využívající platformu Windows. Jedná se o SERVER1 a TERMINÁL. Tyto servery jsou spravovány formou outsourcingu, firmou Gosvo, s.r.o., která zajišťuje pravidelný servis a technickou podporu jak vlastních serverů, tak programů na nich nainstalovaných. Další 2 servery (EMAIL, INTRANET) jsou postaveny na běžných PC s platformou Linux, o které se stará jeden pracovník IT. Servery jsou umístěny v účetním archivu. Tato místnost je odemčená a volně přístupná

Každý server je zálohován proti výpadku proudu svým záložním zdrojem (UPS), dimenzovaným na minimální dobu zálohy 15min. Záložní zdroje nejsou se servery propojeny komunikačním rozhraním, tudíž je neinformují o výpadku napětí a nedojde tak ke korektnímu zavření programů a operačního systému.

1.2.2.1 Server SERVER1

Tento server slouží jako aplikační a databázový server pro informační systém ByznysWin. Server je postaven na značkovém hardwaru od firmy IBM, pro ochranu dat je použit hardwarový RAID1 a pro spolehlivější chod redundantní zdroj. Je spravovaný externí společností. Má nainstalován operační systém Microsoft Small Business Server Premium a pro databázi využívá MS SQL. Autentizace přístupu k poskytovaným službám probíhá pomocí ověřovacího protokolu Kerberos. Přístup do informačního systému je zabezpečen pomocí uživatelského jména a hesla.

1.2.2.2 Server TERMINÁL

Slouží jako terminálový server pro dceřinné společnosti k přístupu do informačního systému ByznysWin. Server je zakoupen od firmy IBM a spravován externí společností. Na serveru je nainstalován operační systém Windows 2003 Server s terminálovým přístupem. Samotné propojení hlavní provozovny a dceřinných poboček je realizováno pomocí sítě Internet. Pro vyšší bezpečnost přenášených dat je použit PPTP tunel. Autentizaci uživatele zajišťuje ověřovací protokol Kerberos, přístup do informačního systému ByznysWin je zabezpečen pomocí uživatelského jména a hesla.

1.2.2.3 Server EMAIL

Slouží jako e-mailový server. Server je postaven na běžném PC se systémem Linux, distribucí Debian. Na serveru je nainstalován mailový systém SendMail 8.12.3, který využívá technologii POP3. Na serveru není nainstalován centrální AntiSpam, ani centrální antivirový systém, který by zprávy před přesunem do počítačové sítě analyzoval a případně je odmítl poslat do lokálních počítačů.

Server běží údajně bez problémů a jeho správu a drobné konfigurace zajišťuje cizí pracovník pomocí vzdáleného přístupu SSH. Příchozí pošta je realizována pomocí protokolu POP3, u kterého je autentizace provedena pomocí uživatelského jména a hesla. Odchozí pošta využívá SMTP poskytovatele internetového připojení.

Nedostatky:

- Systém nebyl od roku 2002 bezpečnostně aktualizován
- Není jasně dáno, kdo server spravuje

1.2.2.4 Server INTRANET

Slouží jako webový server s hypertextovým preprocesorem PHP a databázovým serverem MySQL pro informační systém Intranet. Server je postaven na běžném PC s platformou Linux.

Aplikace firemního intranetu je přístupná pomocí internetového prohlížeče. Každý uživatel přistupuje do systému pod svým uživatelským jménem a heslem, pro které má nastaven určitý stupeň oprávnění jednotlivých modulů. Z vnější sítě je přístup k webovému rozhraní realizován pomocí šifrovaného připojení https.

O samotný hardware se stará firma vlastními silami. Funkčnost systému a technickou podporu zajišťuje externí firma IT Studio, s.r.o. Využívá k tomu samotnou aplikaci Intranet, přístup k FTP protokolu a vzdálený přístup pomocí SSH.

1.2.3 Pracovní stanice

Firma má ve své provozovně celkem 22 pracovních stanic a 8 notebooků. Společnost nevyužívá systémového řešení od jedné firmy, vlastní zařízení od různých dodavatelů. Stáří hardwaru je přibližně 1 až 3 roky. Firma udržuje na skladu minimálně 1 náhradní počítač pro případ poruchy některého PC. O chod pracovních stanic se stará jeden pracovník IT.

Na všech PC a NB jsou nainstalována Windows XP SP2. Proti virům jsou chráněna antivirovým programem NOD 32 zakoupeným jako multilicence. Tento antivirový program si sám automaticky aktualizuje svoji virovou databázi pomocí Internetu. Na počítačích je zapnuta standartní brána firewall systému Windows. Ve firmě se neeviduje, jaké programy jsou nainstalovány na jednotlivých počítačích. Neexistuje ani správa zakoupených licencí.

Software nainstalovaný na jednotlivých počítačích se liší podle pracovní pozice, kterou daný uživatel vykonává. Mezi nejrozšířenější programy patří MS Office, InfoMapa a ByznysWin. V rámci softwarového auditu byly nalezeny nelegální programy, které nainstalovali samotní uživatelé, aniž by je potřebovali pro vykonávání své práce.

Jakýkoli počítač připojený do vnitřní sítě má volný přístup k síti Internet a k e-mailovému a intranetovému serveru. Počítače, které jsou připojeny do domény a jsou autorizovány ověřovacím protokolem Kerberos mají navíc přístup k informačnímu systému ByznysWin a ke sdíleným souborům umístěným na ostatních počítačích v doméně.

Nedostatky:

- Neexistuje evidence poruch
- Nejsou definovány pravidla pro používání SW
- Neexistuje směrnice pro přístup k počítači
- Nejsou definovány pravidla pro přístup do firemní sítě a sítě Internet
- Neexistuje plán obnovy počítačů
- Neexistuje správa licencí SW produktů
- Na počítačích jsou nelegálně nainstalovány pro práci nepotřebné programy

1.3 Informační systémy

Firma Top Moravia Q, s.r.o. si nechala od externích firem zavést dva informační systémy.

1.3.1 ByznysWin

Aplikace ByznysWin slouží pro vedení účetnictví, evidenci majetku, skladové hospodářství a plánování rozvozu. Přístup do aplikace je zabezpečen pomocí uživatelského jména a hesla. Každý uživatel má nastavena oprávnění k jednotlivým modulům.

Aplikace ByznysWin je provozována a spouštěna na vlastním serveru SERVER 1. Aplikace uložené na jednotlivých počítačích pracují přímo s daty uloženými v databázi na serveru. Prostřednictvím serveru TERMINAL 1 je zprostředkována dceřinným firmám služba Terminal Services.

O chod aplikace se stará externí firma Gosvo, s.r.o., která zajišťuje stálou dostupnost aktuální kompilace systému, HotLine telefonní podporu a správu serverů a aplikací. Pro komunikaci s touto firmou byl jmenován jeden odpovědný pracovník. Firma se zavazuje k přijmutí problému a jeho lokalizaci do 24 hodin od písemného nahlášení a vyřešení do 7 pracovních dnů.

K tomuto systému má firma k dispozici všechny důležité materiály popisující předimplementační přípravu, nastavení systému, popis specifických úprav, předávací protokol, evidenci poruch, smlouvu o údržbě, záruční podmínky a garance.

1.3.2 Intranet

Aplikace firemního intranetu je přístupná pomocí internetového prohlížeče. Slouží pro hlášení obchodníků, vzdálený přístup manažerů k analýzám a statistikám, vystavování firemních aktualit a směrnic pro zaměstnance. Každý uživatel přistupuje do systému pod svým uživatelským jménem a heslem, pro které má nastaven určitý stupeň oprávnění jednotlivých modulů.

Aplikace Intranet je provozována a spouštěna na vlastním webovém serveru INRANET s hypertextovým preprocesorem PHP a databází MySQL. Přístup do systému je pomocí internetového prohlížeče. Přístup z vnější sítě je realizován pomocí šifrovaného připojení https. Veškerá data jsou uložena v databázi na serveru.

Firma již několikrát úspěšně provedla obnovu dat ze zálohy. Obnova musela být provedena kvůli neodborné změně nastavení konstant používaných pro výpočty v systému Intranet.

K tomuto systému nemá firma k dispozici materiály popisující systém a implementaci specifických požadavků, uživatelský návod, protokol o předání, ale pouze smlouvu o údržbě a záručních a garančních podmínkách.

Nedostatky:

- K systému neexistuje uživatelská příručka
- K systému nebyl dodán popis implementace specifických požadavků

1.4 Data

Jelikož se firma zabývá širokým spektrem služeb, a to od samotné výroby až po prodej koncovým zákazníkům, vzniká při každodenní činnosti velké množství dat. Tato data mají různou důležitost a citlivost. V rámci dotazování s pracovníky firmy jsem zjistil, že pracují s následujícími typy dat:

- Ve formě databáze IS ByznysWin:
    - Účetnictví (faktury, platební deníky, mzdové výměry, bankovní operace)
    - Skladové hospodářství
    - Zakázky
    - Databáze zákazníků
    - Databáze velkoobchodních odběratelů a dodavatelů
- V IS Intranet:
    - Denní hlášení obchodníků o prodeji
    - Analýzy a statistiky
    - Směrnice
    - Aktuality
- Dokumenty na PC:
    - Sestavy dat (plány rozvozů, evidence majetku,…)
    - DTP grafika (propagační letáky, katalogy)
    - Analýzy (vyhodnocování telemarketingu a přímého prodeje)
    - Pracovní materiály (reklamace, sekretariát,…)
    - Materiály volně šiřitelné (tiskové zprávy, informace o výrobcích, ceníky)
    - Technologické postupy při výrobě
    - Dodavatelské a odběratelské smlouvy
    - Účetní výkazy, daňová přiznání
    - Emaily, vč. příloh
    - Adresáře kontaktů

Většina těchto materiálů existuje pouze v elektronické podobě, některé z nich i v tištěné. Přístup k informacím v IS ByznysWin a Intranetu je zabezepčen pomocí uživatelského jména a hesla, pro které má každý zaměstnanec nastaven určitý stupeň oprávnění. U sdílených dokumentů na PC není nijak specifikováno, kdo má oprávnění s jednotlivými typy dat pracovat. V některých případech uživatelé sdílí celý diskový oddíl C.

Dokumenty jednotlivých uživatelů můžeme rozdělit na 2 podkategorie;

- Dokumenty, které se po vytvoření již nemění
- Dokumenty, které se každý den aktualizují – jedná se zejména o plány rozvozů, analýzy a evidence, se kterými denně pracuje tým lidí. Tyto dokumenty jsou převážně sdílené a jsou významnou součástí pracovního postupu některých zaměstnanců.

V následující tabulce shrnuji, jakým způsobem jsou zavedena ochranná opatření proti ztrátě firemních dat.

Tabulka 2: Ochrana dat před zničením

Kategorie dat	Ochranná opatření	
	redundance HDD	zálohování
DB ByznysWin	RAID1	denní úplné (posledních 7dní)
DB Intranet	ne	dodavatelsky
dokumenty uživatelů	ne	ne

Cena firemních dat se stanovuje na základě odhadu velikosti škody, kterou by způsobilo vyzrazení a zneužití dat, jejich nedostupnost a případné zničení. Hodnota se odvozuje pro každé riziko zvlášť.

1.4.1 Archivace dat

Ve firmě se vyskytují celkem 3 druhy dat – patří mezi ně zejména databáze informačních systémů ByznysWin, Intranet a dokumenty vytvořené uživately.

Osobní počítače uživatelů nejsou nijak zálohovány, v případě havárie to znamená, že uživatel přijde o veškeré dokumenty, e-maily a další data, která nejsou směřována na server nebo do informačního systému. V některých případech se může jednat o podstatné informace, např. smlouvy, profesionální DTP grafika, propagační materiály, analýzy, reporty, evidence, atd.

Každou noc je provedena záloha databáze ByznysWin na externí HDD. K dispozici je vždy posledních 7 záloh databáze. Vedení firmy považuje tyto data za nejcennější a klíčová pro chod firmy, proto se rozhodlo nemít tyto data umístěná na jednom fyzickém místě. Externí disky jsou dva, kdy jeden je připojen k serveru a druhý odnesen pracovníkem IT. Jednou týdně se tyto disky obměňují. Nastavení systému a ostatní data na serveru jsou zálohovány s možností vrácení zpět obden. Zálohování serveru TERMINÁL není prováděno, jelikož neobsahuje žádná data. Tento server pouze zprostředkovává přístup dceřinných společností k datům na hlavním serveru SERVER1.

Zálohu systému Intranet zajišťuje externí firma IT Studio, s.r.o., která každý týden stáhne data pomocí sítě Internet na své servery.

Nedostatky:

- Nejsou zálohovány uživatelské dokumenty
- Nikdy nebyla vyzkoušena funkce obnovy dat DB ByznysWin
- Zálohování Intranetu je prováděno pouze dodavatelsky
- Neexistuje směrnice pro zálohování

1.5 Uživatelé

Uživatelé mají v MS Windows nastavená práva Správce počítače, to znamená, že mohou nainstalovat jakýkoliv program bez příslušné licence, a to i škodlivý, či neúmyslně svojí nevědomostí poškodit funkčnost systému. V rámci zvyšování kvalifikace uživatelů proběhlo pouze školení pro práci v informačním systému ByznysWin a v intranetovém systému. Školení o bezpečnostních zásadách při práci s počítačem neproběhlo.

Na pracovních stanicích je logováno přihlášení uživatelů do místní sítě. Spouštění programů a přístupy uživatelů na síť Internet logovány nejsou. Informační systémy ByznysWin a Intranet mají vlastní logovací soubory, ve kterých jsou zaznamenávány všechny uživatelem provedené změny.

Nedostatky:

- Uživatelé mají v MS Windows práva Správce počítače
- Není prováděno bezpečnostní školení uživatelů
- Soubory uživatelů nejsou zálohovány

1.6 Bezpečnostní politika, směrnice, předpisy

Ve firmě není vytvořena bezpečnostní politika, neexistují žádné psané směrnice pro práci s počítačem, plány zálohování, havarijní plány, plány obnovy a opravy hardware.

Nepsaná pravidla pro práci s počítačem jsou průběžně sdělována na poradách. Jedná se většinou o aktuální problémy, např. zákaz stahování nelegálních programů, používání komunikačního programu ICQ, zákaz používání sítě Internet k vlastním potřebám, u koho řešit vyskytlý problém, atd…

Jeden pracovník IT má na starosti chod pracovních stanic, e-mailového a intranetového serveru, zálohování databáze IS ByznysWin a nákup nového hardware a software. Chod informačního systému ByznysWin a jeho serveru a terminálu je ošetřen dodavatelskou smlouvou.

1.7 Analýza rizik

Vzhledem k rozsahu problematiky zabezpečení informačních systémů jsem se zaměřil pouze na nalezení hrozeb působících na firemní data. Při stanovení pravděpodobnosti uskutečnitelnosti hrozby na jednotlivé skupiny firemních dat jsem vycházel z analýzy současného stavu zabezpečení počítačové sítě.

Tabulka 3: Zranitelnost dat vůči hrozbám

Hrozba	Zranitelnost dat		
	DB ByznysWin	DB Intranet	dokumenty uživatelů
Selhání dodávky energie	1	1	3
Krádež	2	2	4
Poškození paměťového média	1	3	5
Chyba zaměstnanců	2	3	4
Škodlivý software	1	2	2
Přístup neautorizovaným uživatelem	2	1	3

(1 - nejmenší zranitelnost, 5 - největší zranitelnost)

Z tabulky je patrné, že firma nemá dostatečné zabezpečení svých dat proti krádeži a chybám zaměstnanců. Nejhůře zabezpečené jsou přitom dokumenty uživatelů.

V následující tabulce jsem za pomocí informací získaných od vedení firmy definoval sílu dopadu hrozeb na jednotlivá data. Pro přehlednost jsem hrozby seskupil do skupin podle dopadu, který zapříčiní.

Tabulka 4: Síla dopadu

Dopad	Síla dopadu na chod firmy		
	DB ByznysWin	DB Intranet	dokumenty uživatelů
Nedostupnost dat	4	1	3
Ztráta dat	5	2	4
Kompromitace dat	5	4	3

(1 - nejmenší dopad, 5 - největší dopad)

Za nejdůležitější informace firma považuje databázi ByznysWin. Pro bezpečný chod firmy jsou důležité i dokumenty uživatelů. Databáze Intranetu je nejméně potřebná pro chod firmy, zato její vyzrazení konkurenci by významně zhoršilo postavení firmy na trhu.

2 Teoretická východiska řešení

V této kapitole popisuji základní pojmy a principy z oblasti počítačové bezpečnosti, z kterých jsem vycházel při návrhu řešení.

2.1 Bezpečnostní politika IT

„Informační systémy se často stávají obětmi útoků různých druhů lidí, kteří chtějí například získat neoprávněnou výhodu z průniku do cizího informačního systému nebo chtějí mít jenom pocit, že jsou tak dobří, že jsou schopni překonat ochrany, které informační systémy chrání. Protože ale nikdy nevíme, jaké úmysly útočník má, musíme se těmto útokům, přesněji řečeno potenciálním hrozbám, bránit. Soustavě opatření na ochranu firemních aktiv v oblasti IS/IT říkáme bezpečnost IS/IT.“ (14, str.65)

Informační systém je bezpečný, pokud data v něm uložená splňují následující kritéria:

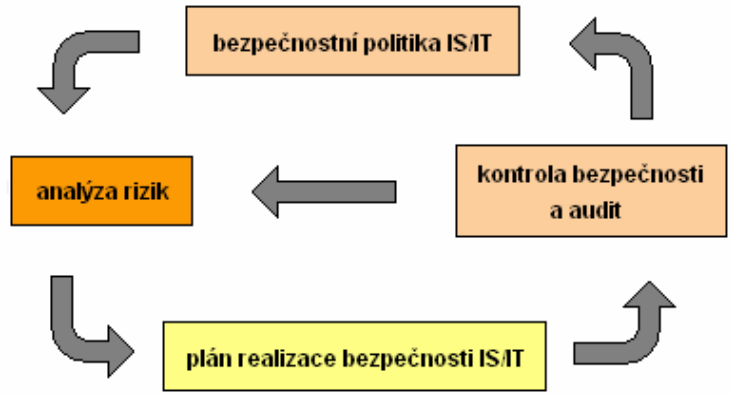
- Důvěrnost (data nemohou číst neautorizovaní jedinci)
- Dostupnost (dostupnost informace na vyžádání oprávněného subjektu)
- Integritu (data nebyla změněna nebo zničena)

Pro bezpečnost informačního systému je nutné, kromě zajištění bezpečnosti dat, se věnovat i následujícím vlastnostem:

- Prokazatelnost prováděných operací (jednotlivé akce mohou být zpětně vysledovány tak, že bude jednoznačně identifikován subjekt, který příslušnou operaci provedl)
- Pravost subjektu (autentizace - potvrzení, že uživatel je prokazatelně tím subjektem, za který se vydává)
- Spolehlivost systému (spolehlivost technických zařízení, jejich zastarávání, pravděpodobnosti selhání, apod.) (14, str.66)

2.1.1 Budování systému bezpečnosti

Při budování bezpečnostní politiky záleží zejména na podnikatelské strategii a určení konkrétní požadované úrovně bezpečnosti. Dalším krokem je vytvoření základní firemní bezpečnostní politiky organizace, na jejímž základě se provede analýza rizik. Proces vybudování a periodické obnovy je znázorněn na obr. č. 3.



Obrázek 3: Budování systému bezpečnosti
Zdroj: (15, str. 86)

2.1.1.1 Bezpečnostní politika organizace

Po definování požadované úrovně bezpečnosti a ujasnění si, jaká aktiva chce firma chránit, vrcholové vedení firmy zpracuje bezpečnostní politiku organizace. V tomto dokumentu jsou stanoveny strategické cíle, způsob jejich dosažení a použité nástroje pro zajištění bezpečnosti IS/IT.

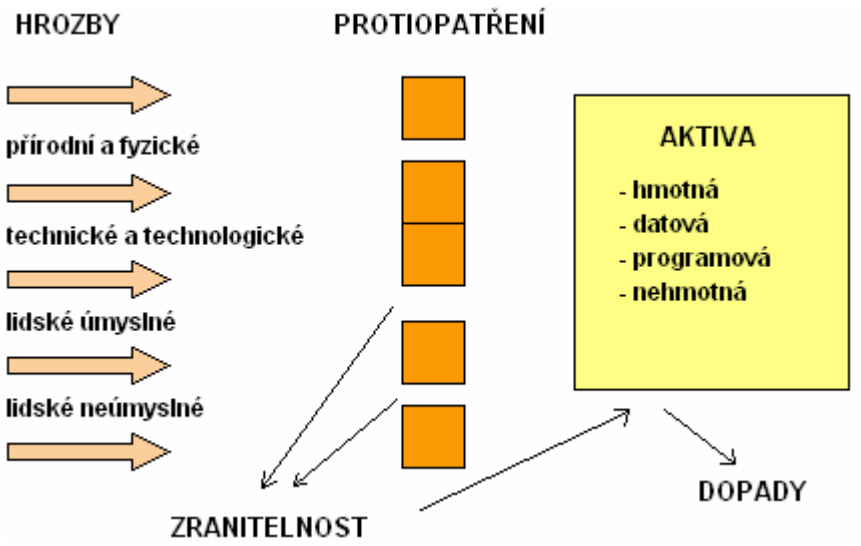
„Vzhledem k tomu, že budování bezpečnosti IS/IT je permanentní proces, je nutné bezpečnostní politiku v pravidelných časových intervalech přehodnocovat a aktualizovat. Za východiska pro změny v bezpečnostní politice jsou obvykle považovány závěry analýzy rizik.„ (15, str. 87)

2.1.1.2 Analýza rizik

Předmětem analýzy rizik je hodnocení ztrát, které mohou vzniknout působením hrozeb na IS/IT. Účinnost této analýzy závisí na kvalitě podkladů, které máme k dispozici a na zkušenostech týmu, který analýzu provádí. Na základě analýzy rizik je pak možné definovat odpovídající protiopatření. Základní východiska a postupy pro provedení analýzy rizik jsou uvedeny v ČSN ISO/IEC 13335 1-5.

2.1.2 Bezpečnostní prvky

V následujících podkapitolách jsou popsány hlavní prvky zapojené do procesu řízení bezpečnosti. Na obr. č. 4 je znázorněna jejich vzájemná souvislost.



Obrázek 4: Schéma zajištění bezpečnosti
Zdroj: (14, str. 66)

2.1.2.1 Aktiva

Aktivum IS/IT lze chápat jako libovolnou část IT/IS, která je pro organizaci dostatečně cenná, aby si zasloužila určitý stupeň ochrany. Požadavky na tuto ochranu jsou ovlivněny zranitelností aktiv při výskytu specifických hrozeb.

Aktivy rozumíme především:

- Hmotná aktiva (počítače, tiskárny, komunikační prostředky, atd…)
- Data (zejména databáze a dokumenty)
- Software
- Nehmotná aktiva (např. image firmy)

2.1.2.2 Hrozby

Hrozba je možnost způsobit potenciální poškození systému, organizace a jejich aktiv. Hrozby mohou mít přírodní, technický nebo lidský původ a mohou být úmyslné a neúmyslné. Všechny hrozby by měly být identifikovány a měla by být odhadnuta pravděpodobnost jejich uskutečnění.

„Převážná většina hrozeb, které poškodí IS/ICT organizace (více jak 50% ze všech), patří do kategorie neúmyslných hrozeb. Také podíl hrozeb zevnitř organizace je významně vyšší než hrozby z vnějšku. Podle některých statistických zdrojů až 98 procent všech bezpečnostních incidentů v organizaci je interního původu.„ (14, str. 67)

2.1.2.3 Zranitelnosti

„Zranitelnosti zahrnují slabá místa v systému, která mohou být hrozbou využita a mohou vést k nežádoucím následkům. Například absence mechanismu řízení přístupu je zranitelnost, která by mohla umožnit výskyt hrozby nežádoucího proniknutí k aktivům a jejich ztrátu.“ (8, str. 12)

2.1.2.4 Dopad

Dopad je důsledek nežádoucího incidentu, kterým došlo k narušení určitých aktiv. Následky mohou mít podobu poškození systému IT, ztráty důvěrnosti, integrity, dostupnosti nebo spolehlivosti. Další, nepřímé následky zahrnují finanční ztráty, ztráty podílu na trhu a poškození image společnosti.

„Měření dopadů umožňuje vytvoření rovnováhy mezi výsledky nežádoucích incidentů a náklady na ochranná opatření sloužící na ochranu před nežádoucími incidenty.“ (8, str. 12)

2.1.2.5 Protiopatření

Protiopatření jsou praktiky nebo mechanismy, které poskytují ochranu před hrozbou, sníží zranitelnost, omezí dopad bezpečnostního incidentu a usnadní obnovu. Existuje několik typů ochranných opatření. Jedná se o ta, která zabraňují a detekují nežádoucí incidenty a ta, která zajišťují obnovu po bezpečnostních incidentech. Mezi opatření působící proti nežádoucím činnostem patří i prevence, zastrašování a zvyšování povědomí o bezpečnosti.

Mezi oblasti ochranných opatření patří:

- Hardware (zálohování, redundance)
- Software (digitální podpisy, antivirové nástroje, monitorování a logování)
- Komunikace (ochranné firewally, šifrování dat)
- Fyzické prostředí (oplocení, uzamčení)
- Personál (školení, směrnice)
- Administrativa (autorizace, kontrola licencí, likvidace hardwaru)

2.1.3 Útočníci

Útok je realizací hrozby. Pokud chceme útočníkovi zabránit v útoku, je nutné znát jeho odbornost a pochopit jeho motivaci. Útočníky můžeme dělit do dvou kategorií, a to na vnější a vnitřní útočníky.

2.1.3.1 Vnější útočník

Vnějším útočníkem je označován člověk, který nemá přímý fyzický přístup k síti. Do firemní sítě přistupuje většinou přes Internet, musí proto zdolat všechny překážky, jako je např. firewall. Vnější útočníky rozdělujeme podle jejich schopností a dostupných prostředků do tří kategorií.

Amatér

Tento útočník má minimální znalosti. Pro útok většinou využívá známé postupy a běžně dostupné nástroje. Pro zabezpečené systémy nepředstavují výrazné nebezpečí, stačí se chránit základními ochrannými prostředky.

Cracker

Tuto skupinu útočníků zná většina lidí pod mylným označením Hacker (což je počítačový specialista či programátor). Počítačový zločinec s podobnými znalostmi se nazývá Cracker. Ten využívá své znalosti o slabém zabezpečení pro osobní prospěch nebo ke kriminálním účelům. Cracker má dobré znalosti z oblasti informačních technologií, ale je omezen finančními prostředky a výpočetním výkonem. Tyto skupiny jsou středně nebezpečné, dokáží proniknout do většiny systémů, ale většina z nich útok detekuje.

Profesionál

Profesionál má vynikající znalosti a disponuje běžně nedostupnými prostředky. Ví, jak jsou jednotlivé systémy chráněny a zná většinu bezpečnostních děr. Jsou schopni se nabourat do většiny systémů, aniž by byli detekováni. Pokud se rozhodnou zaútočit na určitou firmu, dokáží způsobit velké škody. Ochrana proti této skupině útočníků je velice nákladná.

2.1.3.2 Vnitřní útočník

Pod pojmem vnitřní útočník si můžeme představit osobu, která má přímý přístup k firemní síti. Jedná se hlavně o zaměstnance, kteří útočí buď z vlastní iniciativy (chce se pomstít zaměstnavateli, výhodně prodat citlivá data konkurenci, atd…) nebo neúmyslně svojí nevědomostí. Tito útočníci nemívají profesionální znalosti informačních systému, proto je snadné se jim bránit.

2.1.4 Organizační aspekty bezpečnosti IT

Bezpečnost IS/IT se týká každého informačního systému a všech zaměstnanců v určité organizaci. Pro zajištění efektivního plnění všech důležitých úkolů je potřeba přiřadit odpovědnosti a pravomoci jednotlivým uživatelům. Ačkoliv každá firma je jinak velká a má specifické organizační schéma, v každé organizaci je nutné pokrýt výkonné a kontrolní role.

2.1.4.1 Kontrolní role

- Vrcholové vedení organizace
    - Deklaruje strategické cíle
    - Formuluje bezpečnostní politiku organizace
    - Pravidelně vyhodnocuje stav bezpečnosti v organizaci
- Auditor bezpečnosti IS/IT
    - Provádí pravidelný audit v oblasti IS/IT podle stanovené metodiky

2.1.4.2 Výkonné role

- Bezpečnostní manažer organizace
  - Provádí aktualizace politiky bezpečnosti IT a bezpečnostních směrnic
  - Koordinuje prozkoumávání incidentů
  - Metodicky vede bezpečnostního manažera IS/IT
- Bezpečnostní manažer IS/IT
  - Zodpovídá za zavedení bezpečnosti IS/IT v organizaci
  - Řeší bezpečnostní incidenty
  - Denně monitoruje implementaci a používání ochranných opatření
- Pracovník IT oddělení
  - Je odpovědný za provozování bezpečnostních funkcí
  - Vyšetřuje a oznamuje bezpečnostní incidenty
  - Zodpovídá za nastavení IS/IT (8, str. 12 – 14)

2.1.4.3 Role v malé organizaci

Pro malé firmy je výhodnější přenechat kontrolní role externí firmě, a to formou outsourcingu. Výkonné role se účelně spojují a přidělují jednomu zaměstnanci (např. role *Bezpečnostní manažer* organizace a *Bezpečnostní manažer IS/IT* zajišťuje jeden pracovník). Vždy je ale nutné oddělit roli *Auditora bezpečnosti IS/IT* od všech ostatních rolí. Pokud firma není dostatečně velká, či nemá k dispozici odpovídajícího zaměstnance, může roli auditora řešit formou outsourcingu některé konzultační firmy.

2.2 Prostředky pro zabezpečení

2.2.1 Firewall

Firewall slouží k řízení síťového provozu mezi sítěmi s různou úrovní zabezpečení. Toto síťové zařízení se používá zejména k ochraně vnitřní firemní sítě před útoky ze sítě Internet. Firewall kontroluje tok dat mezi sítěmi a podle nastavených pravidel tento pohyb řídí.

2.2.2 Antivir

Antivir je počítačový program, který slouží k detekci a odstranění škodlivého softwaru (viry, trójské koně, spyware,…). Pro zabezpečení počítače je kromě výběru vhodného antivirového programu důležité aktualizovat databázi počítačových virů.

2.2.3 VPN (Virtual Private Network)

Pokud má firma svá pracoviště na více místech a potřebuje je propojit, má dvě možnosti. První je vybudování vlastní sítě WAN. Tato varianta je finančně velice náročná, protože vyžaduje vybudování vlastních fyzických linek. Proto organizace využívají druhou variantu, u které své pobočky propojují pomocí celosvětové sítě Internet. Tato varianta využívá širokopásmové připojení do veřejně přístupné sítě Internet a v poslední době se stala cenově dostupnou a dostatečně rychlou. Pro zabezepčení přenášených dat se komunikace mezi jednotlivými entitami provádí pomocí technologie VPN. VPN je prostředek k vytvoření bezpečného komunikačního kanálu mezi několika entitami, umístěnými na různých místech. Komunikace je šifrována a tak při přenosu přes síť Internet zabezpečena. Dá se říci, že se na otevřené síti vytvoří mezi dvěma entitami tunel.

VPN se používá k různým účelům, jednak jako propojení dvou vzdálených sítí (propojení více poboček do jedné virtuální sítě), nebo připojení jednoho PC do vzdálené sítě (např. zaměstnanec pracující z domova se připojí do firemní sítě a využívá poskytované služby).

2.2.4 Řízení přístupu

Řízení přístupu určuje, který uživatel má oprávnění přístupu k určitému objektu (soubor, databáze,…). Řízení přístupu by mělo být realizováno podle principu „nejmenších privilégií“. Ten udává, že nejdříve všem uživatelům zakážeme přístup ke všem objektům a poté jim postupně povolujeme ty objekty, které pro svoji pracovní pozici bezpodmínečně potřebují. Žádný uživatel by neměl mít přístup k objektům, ke kterým ho nepotřebuje.

2.2.4.1 Active Directory

Active Directory je databáze síťových objektů v síti MS Windows. Adresářová služba Active Directory umožňuje efektivně uspořádat síťové prostředky do hierarchické struktury objektů (uživatelé, služby, prostředky), o kterých poskytuje informace a spravuje bezpečnostní politiku. Je založen na ověřovacím protokolu Kerberos a LDAP.

2.2.4.2 Doména

„Doména je logické seskupení síťových počítačů, které sdílejí centrální databázi síťových údajů (uživatelské účty, počítače, informace o zabezpečení). … Po přihlášení k doméně máme k dispozici všechny zdroje serveru (definované naším uživatelským účtem).“ (5, str. 68)

2.2.4.3 Group Policy

Group Policy (zásady skupin) umožňují s pomocí Active Directory administrátorům centrálně spravovat uživatele a počítače. Group Policy je jedním z nejužitečnějších nástrojů při budování bezpečnostní politiky. Umožňuje každé skupině či jednotlivému uživateli připojeného do domény nastavit oprávnění přístupu k určitým objektům. Např. tak můžeme jednoduše nastavit, že žádný uživatel ze skupiny účetního oddělení si nenainstaluje nový program.

2.3 Ochrana dat

Data jsou nejdůležitějším aktivem každé firmy. Přestože je pomocí nejmodernějších technologií chráníme proti zneužití, je nutné je zabezpečit před havárií serveru. Fyzickou ochranu můžeme rozdělit do dvou kategorií, a to do automatické redundance pomocí diskových polí a ručního zálohování dat.

2.3.1 Disková pole

Pro zvýšení výkonu serverů a odolnosti vůči chybám nebo ztrátě dat se pevné disky zapojují do diskových polí, a to pomocí metody RAID (Redundant Array of Independent Disks). Vyšší bezpečnosti je dosaženo díky redundanci (nadbytečnosti) uložených dat. Při havárii se z těchto redundantních dat dopočítají chybějící údaje.

Existuje celkem šest typů polí, prakticky se používají tři typy:

- RAID 0 (prokládání)
    - Data se rozdělují mezi několik disků
    - Vyšší kapacita
    - Nezvyšuje bezpečnost
- RAID 1 (zrcadlení)
    - Data se současně zapisují na více disků, jeden disk je úplnou kopií druhého
    - K uložení dat je potřeba dvojnásobná kapacita
    - Data jsou 100% redundantní
- RAID 5 (prokládání s redundancí)
    - Data jsou rozdělována mezi více disků
    - Na disky se střídavě ukládají redundantní data
    - Havarovaný disk je možné vyměnit, pole samo zrekonstruuje chybějící data
    - K uložení dat je potřeba N+1 disků (jeden disk zaberou redundantní data)

2.3.2 Zálohování

Jelikož nejdražším aktivem každé firmy jsou data, zabezpečují se kromě redundance pomocí diskových polí i archivací na externí média. Tím data ochráníme např. před krádeží a živelnou pohromou. Nemalou výhodou je i možnost obnovit data, která uživatel omylem smazal, či nesprávně upravil.

2.3.2.1 Plán zálohování

Než vybereme vhodnou zálohovací strategii, musíme si rozmyslet několik důležitých aspektů. Zejména co budeme zálohovat a jak často. Je totiž zbytečné zálohovat soubory, které můžeme lehce obnovit např. z instalačního CD. Zálohujeme tedy hlavně data (databáze účetnictví, dokumenty uživatelů, konfigurační soubory, atd…), čímž ušetříme místo na záložním médiu. Dále se musíme rozhodnout, jak často budeme zálohovat. Frekvence zálohování závisí na tom, jak často se data mění. Pokud jednou denně, zálohujeme tedy každý (popř. pracovní) den. Pokud se mění jednou týdně, zálohujeme jednou za týden.

2.3.2.2 Typy zálohování

Podle velikosti zálohovaných dat a množství prováděných změn můžeme vybrat jeden ze tří základních způsobů zálohování:

- Normální (úplné)
  - Zálohují se všechny soubory
  - Záložní kopie má velký objem dat
- Přírůstkové
  - Zálohují se soubory změněné od provedení poslední zálohy
  - Záloha má menší objem dat
  - Pro obnovu dat je nutná poslední úplná záloha a všechny následující přírůstkové
- Rozdílové
  - Zálohují se pouze soubory změněné od provedení poslední úplné zálohy
  - Pro obnovení je potřeba poslední úplná záloha a jedna rozdílová

2.3.2.3 Zálohovací média

V dnešní době existují různé druhy zálohovacích médií. Rozlišují se technologií zápisu, kapacitou, rychlostí a trvanlivostí na nich uložených dat. V malých a středně velkých firmách je nejrozšířenější zálohování na pásky nebo pevné disky. Vždy je ale bezpečnější zálohovat na vyjímatelné médium, které můžeme ukládat mimo budovu. Zamezíme tak ztrátě dat způsobené např. vykradením či živelnou pohromou. Všechny záložní kopie by jsme měli řádně popisovat a evidovat, abychom věděli z jakých médií provést obnovu a která média můžeme přepsat novou zálohou.

2.3.2.4 Obnova dat

Při výběru zálohovacího softwaru vybíráme nejen podle požadovaných funkcí potřebných pro zvolený systém, ale i podle toho, zda nám program umožní kontrolu zálohovaných dat. Chceme-li si být jisti, že zálohovací systém je správně nakonfigurován, musíme namátkově testovat funkčnost zálohy. Může se totiž lehce stát, že jsme zálohovali jiná data než jsme chtěli, popř. nejsme schopni data obnovit, např. z důvodu šifrování, uložení neúplných dat či chybou zálohovacího média. V některých případech je důležitá i rychlost, s jakou jsme schopni data či operační systém včetně konfigurace aplikačního prostředí obnovit. Pokud nejsme z jakéhokoliv důvodu schopni provést obnovu dat, jsou všechny prostředky vynaložené na zálohování zbytečné.

3 Návrh řešení

V závěru analýzy současného stavu zabezpečení IS/IT ve firmě Top Moravia Q, s.r.o. jsem analyzoval hrozby, které mohou negativně působit na firemní data. Přihlížel jsem k uskutečnitelnosti hrozby v současných podmínkách a k síle dopadu na chod firmy. V této kapitole navrhuji řešení shrnuté do dvou logických celků. V prvním vybírám vhodná technická protiopatření, v druhém organizační. V závěru kapitoly zhodnotím efektivitu navržených změn.

Tabulka 5: Protiopatření vůči jednotlivým hrozbám

Hrozba	Významně zranitelná data	Protiopatření
krádež	ByznysWin, Intranet, Dokumenty	ochrana fyzického přístupu k serverům
selhání dodávky energie	-	-
poškození paměťového média	Intranet, Dokumenty	zálohování
chyba zaměstnanců	Intranet, Dokumenty	zálohování (archivace), směrnice
přístup neautorizovaným uživatelem	Dokumenty	řízení přístupu (Active Directory, Group Policy)

Požadavky firmy Top Moravia Q, s.r.o.:

- Data zálohovat na lehce přenositelná média
- Znemožnit zaměstnancům instalovat nelegální software

Cíle:

- Zajištění důvěrnosti a integrity DB Intranet
- Zajištění důvěrnosti, dostupnosti a integrity DB ByznysWin
- Zajištění důvěrnosti a integrity uživatelských dokumentů

3.1 Technické prostředky ochrany dat

V této části popisuji, pomocí jakých technických protiopatření chci snížit míru dopadu nalezených nejrizikovějších hrozeb.

3.1.1 Ochrana fyzického přístupu

Serverovna je srdcem celé firmy, nacházejí se zde veškerá data společnosti. Současný stav umístění serverů a aktivních prvků ve společné místnosti s účetním archivem není bezpečný. Prostor se servery by neměl být volně přístupný jako doposud, nýbrž by měl být zabezpečen proti přístupu nekompetentních osob. Navrhuji tedy fyzicky oddělit prostor archívu a prostor pro servery.

Optimálním řešením, vzhledem k dispozičním možnostem dané budovy, je vybudování nehořlavé příčky s uzamykatelnými dveřmi v prostorách současného archivu. V tomto novém prostoru doporučuji vzhledem k jeho velikosti a tepelném výkonu serverů zajistit klimatizaci, která sníží teplotu vzduchu ze současných 24°C (měřeno dne 20.3.2008) na optimálních 18°C.

3.1.2 Ochrana logického přístupu

Během analýzy jsem zjistil, že firma nemá vytvořenou směrnici o klasifikaci dat. Může se tak stát, že k citlivým datům mají přístup i neautorizovaní uživatelé. Navrhuji tedy nakonfigurovat Active Directory a připojit všechny uživatele do domény. Na všech počítačích se nastaví směřování všech dokumentů a důležitých dat na server, kde by byly tyto data centrálně uloženy. Pro data, která jsou sdílena určitým týmem lidí, se vytvoří síťové jednotky. K těmto jednotkám budou mít přístup pouze ty osoby, které s daty bezpodmínečně pracují.

Další výhodou připojení PC do domény a uložení uživatelských dokumentů na serveru je jednodušší zálohování uživatelských dat.

Při přechodu na přihlašování uživatelů do domény je nutné současné licence Windows XP Home nahradit systémem Windows XP Professional. Windows XP Home totiž není možné připojit k centrálně spravované doméně (serveru), kde by byla uplatňována centrální politika bezpečnosti.

3.1.2.1 Group Policy

Uživatelé mají v MS Windows nastavená práva Správce počítače. Prakticky tak mohou nainstalovat jakýkoliv program, a to i škodlivý nebo nelegální, či neúmyslně svojí nevědomostí poškodit funkčnost systému.

K spuštěnému Active Directory doporučuji zavést a nakonfigurovat Group Policy. Tímto krokem se zabrání nejen instalování potenciálně nebezpečných programů, ale zvýší se i bezpečnost celého systému. Každému uživateli se podle pracovního zařazení přiřadí určité oprávnění (např. kam mají přístup, které programy mohou spustit, nezmění nastavení počítače, nenainstalují si žádný SW, atd…). Vybraný pracovník by měl administrátorský účet, kterým by počítače spravoval.

3.1.3 Zálohování dat

V současné době firma zálohuje databázi IS ByznysWin na externí disk, k dispozici má zálohu za posledních 7 dní. Databázi systému Intranet zálohuje externí firma. E-maily a data uživatelů zálohovány nejsou. Je tedy nutné navrhnout zálohovací strategii úměrnou velikosti ukládaných dat.

Tabulka 6: Velikost zálohy

data	velikost [GB]
IS ByznysWin	25
IS Intranet	1
Uživatelská data (30 uživatelů)	90
CELKEM	**116**

Vzhledem k hodnotě dat doporučuji zavést systémové řešení, ve kterém by se všechna data zálohovala po dnech: pondělí – čtvrtek, dále po týdnech: 5 pátků a po měsících: leden – prosinec. Operační systémy a konfigurace serverů (celkem 15GB) by byly zálohovány pouze v pátky.

Jako řešení, vhodné pro vybraný systém zálohování, můžeme uvažovat provádění zálohy na síťové disky, nebo pomocí páskové mechaniky. Jelikož cenu určuje zejména velikost zálohy, která je s rezervou 200GB, vychází jako optimální řešení použití páskové mechaniky LTO2 a 25ks 200GB pásek. Páskovou mechaniku je možné osadit do současného serveru SERVER1, čímž se sníží náklady. Pásky s denními zálohami doporučuji umístit do firemního trezoru, pásky s týdenními a měsíčními zálohami do jiné budovy.

Pro kvalitní, ale hlavně použitelné zálohování je kromě vhodného HW vybavení potřeba vybrat i odpovídající SW, který nám umožní kontrolovat provádění jednotlivých záloh a zejména namátkové testování funkčnosti zálohování. Tedy zda pomocí zálohy je možno provést plně funkční obnovu dat a nastavení systému. Navrhuji použít SW řešení ARCserve backup, který (mimo jiné) obsahuje nástroje pro zálohu souborového serveru, MS SQL databáze a Exchange serveru. Tento produkt umožňuje i správu obnovy dat a použití jakékoliv ukládací technologie (HDD, páska).

3.1.3.1 Náklady na obnovu dat

Při výpočtu nákladů na obnovu dat jsem vycházel z dotazníku, ve kterém každý uživatel vyplnil, kolik hodin denně aktivně vytváří uvedená data. Pro přesnější vypočtení reálných nákladů rozděluji obnovu dat na dvě kategorie. První je obnova dat z materiálů, které jsou k dispozici i v papírové formě. Jedná se zejména o účetní doklady. Tuto obnovu může provádět i brigádník bez zkušeností v daném oboru. Proto hodinovou taxu za obnovu dat z papírové zálohy ohodnocuji 70Kč/hod. Druhou kategorií jsou elektronická data, která jsou kreativně vytvářena odbornými pracovníky a jsou vedena pouze v elektronické podobě. Náklady na obnovu těchto dat tedy vyčísluji podle mzdových nákladů na jednotlivé zaměstnance. Všechny získané údaje jsou přehledně shrnuty v tabluce č.7 *Náklady na obnovu dat*. Jednotlivé uživatele jsem pro přehlednost shrnul podle jejich pracovního zařazení do logických celků.

Tabulka 7: Náklady na obnovu dat

pracovní zařazení	počet uživatelů	tvorba el. dat (hodin denně)				z toho i v papírové formě	cena obnovy dat z papírové zálohy [Kč]	cena obnovy dat z kreativní činnosti [Kč]
		ByznysWin	Intranet	dokumenty	CELKEM			
Plánování	4	0	4	11	15	13	910	500
Grafik	1	0	0,2	5	5,2	3,5	245	510
Obchod	6	0	2,8	16	18,8	12	840	4 760
Fakturace	8	42	0,5	4,5	47	38	2 660	1 350
Vedení společnosti	3	1	1,5	5	7,5	2	140	4 400
Sklad	3	3	0	0	3	3	210	0
Reklamace	2	2,5	0,2	3	5,7	4	280	340
Recepce	3	0	0,3	1,3	1,6	1	70	108
Obchodní zástupci	30	0	15	0	15	15	1 050	0
						CELKEM:	**6 405**	**11 968**

Celkové náklady na obnovu dat vytvořených v jeden pracovní den jsou tedy 18.373,- Kč. Týdenní potom 91.865,- Kč. V těchto nákladech ovšem není vyčíslen ušlý zisk, o který firma přijde v důsledku časového prodlení a neaktuálních dat.

3.2 Bezpečnostní politika

V současné době ve firmě neexistují žádné pevně dané podmínky při práci s informačními technologiemi. Pokud uživatel provede bezpečnostní hrozbu, ať úmyslnou, či neúmyslnou, tak podle stávajících podmínek mu nehrozí žádné sankce. Tento stav považuje vedení firmy za kritický, proto v rámci návrhu zabezpečení IS/IT definuji základní aspekty bezpečnostní politiky.

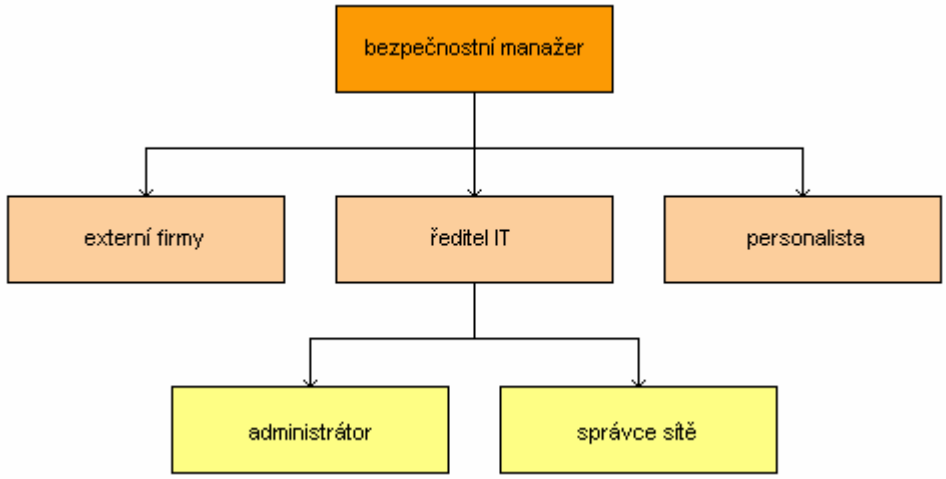
Podle mnou navržené bezpečnostní politiky vedení firmy určí, kteří pracovníci přejímají které role v systému řízení bezpečnosti. Každá role bude mít vymezeny své povinnosti. Po splnění všech těchto dílčích povinností se postupně zavede bezpečnostní politika (jak po SW/HW stránce, tak po stránce uživatelské). Poté budou jednotliví zaměstnanci seznámeni s novými pravidly a povinnostmi. Po 6 měsících se provede nový bezpečnostní audit pro kontrolu, zda je tato bezpečnostní politika optimální a jestli nenastaly nějaké změny, které mají dopad na bezpečnost celého systému.

3.2.1 Role

V systému řízení bezpečnosti definuji tyto role:

- **Bezpečnostní manažer (CISO)**
  - kontroluje plnění bezpečnostních předpisů
  - schvaluje smlouvy s externími společnostmi
  - je zodpovědný za řízení krizových plánů
- **Ředitel IT (CIO)**
  - stanovuje pravidla pro práci s výpočetní technikou
  - monitoruje a kontroluje logovací soubory
- **Administrátor**
  - spravuje licence SW produktů
  - spravuje oprávnění jednotlivých uživatelských účtů
  - je zodpovědný za zálohování dat
  - je zodpovědný za aktualizaci bezpečnostních záplat SW produktů

- **Správce sítě**
  - je zodpovědný za HW vybavení, jeho funkčnost a nákup
  - je zodpovědný za nastavení firewallu
- **Personalista**
  - organizuje školení o bezpečnosti IS/IT
- **Externí firmy**
  - provádí průběžný bezpečnostní audit
  - zajišťují chod IS ByznysWin a IS Intranet



Obrázek 5: Role v systému řízení bezpečnosti

3.2.2 Směrnice

V následujících podkapitolách popíši u jednotlivých směrnic co musí bezpodmínečně obsahovat, kdo je vytvoří, kdo se jimi musí řídit, kdo kontroluje správnost a celistvost směrnic a jaké jsou sankce v případě nedodržení určených pravidel. Sankce slouží zejména jako represe, nikoliv jako náhrada za vzniklou škodu. Mnou navržené sankce jsou orientační a budou uplatňovány formou nepřipsání pohyblivé složky mzdy.

3.2.2.1 Pravidla přístupu do serverové místnosti

Popis: V této směrnici bude popsáno, jakým způsobem je zajištěna místnost se servery proti vniknutí nekompetentních osob, kdo má do této místnosti přístup a jakým způsobem bude prováděna evidence přístupů.
Vytvoří: Ředitel IT
Kontroluje: Bezpečnostní manažer
Řídí se: všichni uživatelé
Sankce: v případě nedodržení směrnice sankce v rozmezí 5.000,- až 10.000,- Kč

3.2.2.2 Směrnice o ukládání a zálohování dat

Popis: Tato směrnice klasifikuje jednotlivá data, vznikající při pracovní činnosti zaměstnanců, a určuje kdo má ke kterým datům přístup. Dále specifikuje systém ukládání a popisování souborů na uživatelských PC, systém zálohování, osoby zodpovědné za konfiguraci zálohovacího SW, výměnu pásek a namátkovou kontrolu funkčnosti obnovení zálohy. Směrnice by měla obsahovat i definici, v jakých podmínkách mají být záložní pásky uloženy a která data se mají zálohovat.
Vytvoří: Administrátor
Řídí se: všichni uživatelé
Kontroluje: Ředitel IT
Sankce: podle závažnosti pochybení sankce až do výše 5.000,-

3.2.2.3 Směrnice o nastavení Firewallu

Popis: Tato směrnice obsahuje pravidla pro nastavení firewallu, včetně specifikace všech služeb a portů spuštěných na jednotlivých serverech.
Vytvoří: Ředitel IT

Řídí se: Správce sítě

Kontroluje: Bezpečnostní manažer

Sankce: v případě nedodržení směrnice sankce až do výše 5.000,- Kč

3.2.2.4 Směrnice o správě uživatelských účtů

Popis: Každý uživatel je přiřazen podle pracovního zařazení do třídy. Každá třída má určitá oprávnění a omezení při používání firemních SW a HW prostředků (např. instalace SW, přístup na internet, intranet, atd…). Směrnice navíc specifikuje, kdo spravuje evidenci oprávnění konkrétních zaměstnanců v určených třídách a jakým způsobem jsou příslušná oprávnění a omezení softwarově zajištěna (např. Group Policy).

Vytvoří: Ředitel IT, Personalista

Řídí se: Administrátor

Kontroluje: Bezpečnostní manažer

Sankce: v případě nedodržení směrnice sankce až do výše 2.500,- Kč

3.2.2.5 Směrnice o správě licencí SW produktů

Popis: Směrnice upravuje základní pravidla pro nákup, instalaci a používání SW produktů. Dále upravuje administrátorská oprávnění na jednotlivých PC a oprávnění uživatelů používat a instalovat SW (podle zařazení do určité třídy). Směrnice obsahuje i specifikaci, jakým způsobem jsou spravovány licence zakoupeného software, kdo je odpovědný za nákup programů včetně aktualizací, správu a průběžný audit licencí.

Vytvoří: Ředitel IT

Řídí se: Administrátor, Uživatelé

Kontroluje: Bezpečnostní manažer

Sankce: sankce až do výše 5.000,- Kč

3.2.2.6 Pravidla práce s výpočetní technikou pro uživatele

Popis: Tato směrnice obsahuje základní bezpečnostní pravidla pro práci s výpočetní technikou, která musí dodržovat všichni uživatelé pracující s informačními technologiemi a systémy firmy Top Moravia Q, s.r.o. Mezi zmíněné uživatele patří nejen zaměstnanci firmy Top Moravia Q, s.r.o., ale i zaměstnanci dceřinných společností, obchodní zástupci a příležitostní brigádníci.

Směrnice musí obsahovat pravidla pro následující kategorie:

- základy práce s výpočetní technikou
- řízení přístupu
- terminálový přístup
- používání SW
- ochrana před škodlivým SW
- elektronická pošta
- používání sítě Internet
- řešení bezpečnostních incidentů

Vytvoří: Administrátor, Ředitel IT

Řídí se: všichni uživatelé

Kontroluje: Bezpečnostní manažer

Sankce: podle rozsahu pochybení, nebo podle výše způsobené škody

3.2.3 Krizové plány

Krizové plány slouží k rychlému vyřešení bezpečnostních incidentů. Jedná se o souhrn postupů a reakcí, jejichž cílem je organizovaně identifikovat a vyřešit vzniklý problém.

3.2.3.1 Plán obnovy po havárii

Popis: Tento plán bude obsahovat postupy, jak jednat v případě zničení HW vybavení, ať už živelnou pohromou, úmyslným poškozením či zestárnutím materiálu. Plán musí obsahovat i náhradní řešení pro co nejrychlejší uvedení výpočetní techniky do funkčního stavu.
Vytvoří: Správce sítě
Řídí se: všichni uživatelé
Kontroluje: Bezpečnostní manažer
Sankce: bez sankcí

3.2.3.2 Plán činnosti po útoku

Popis: Plán obsahuje postupy, jak jednat v případě napadení informačních systémů. Určuje, kdo obnoví provozuschopnost IS a kdo provede řešení vzniklého incidentu včetně nalezení viníka. O vzniklé události musí být vyhotovena zpráva a dále návrh preventivních opatření zvyšující úroveň bezpečnosti.
Vytvoří: Administrátor
Řídí se: všichni uživatelé
Kontroluje: Bezpečnostní manažer
Sankce: bez sankcí

3.2.4 Outsourcing

Popis: Určený pracovník zajišťuje přehled externích firem, které se podílí na chodu informačních systémů a technologií. Schvaluje smlouvy, kontroluje jejich plnění a je pověřen jednáním se zástupci těchto firem.

Zajišťuje: Ředitel IT

Kontroluje: Bezpečnostní manažer

Sankce: bez sankcí

3.2.5 Kontrola ochranných opatření

Jelikož se v průběhu životního cyklu firmy mění požadavky na fungování informačních systémů a vznikají nové a nové technologie, je nutné zavedenou bezpečnostní politiku periodicky obnovovat.

3.2.5.1 Prověřování bezpečnosti IS/IT

Popis: Předmětem kontroly je identifikovat aktuální hrozby a analyzovat příslušná rizika. Na tomto základě se specifikují příslušná protiopatření a upraví, popř. vytvoří nová bezpečnostní politika IS/IT. Součástí je i kontrola logovacích souborů a průběžné testování bezpečnosti.

Zajišťuje: Externí firma, Ředitel IT

Sankce: v případě neplnění povinností sankce do výše 20.000,- Kč

3.2.6 Školení

Popis: Mnohdy nejslabším článkem v oblasti zabezpečení IS/IT je koncový uživatel. Je tedy nutné provádět školení zaměstnanců, na kterém se zvýší bezpečnostní povědomí uživatelů. Uživatelé by měli být vyškoleni zejména v oblasti: používání bezpečných hesel, škodlivého SW, práce s důvěrnými daty, používání elektronické pošty, atd…

Zajišťuje: Bezpečnostní manažer, Personalista

Sankce: v případě neplnění povinností sankce v rozmezí 5.000,- až 10.000,- Kč

3.3 Zhodnocení efektivity navržených změn

V následující tabulce uvádím přehled všech investic do navrhnutých protiopatření. V jednotlivých podkapitolách poté zhodnotím efektivitu navrhnutého řešení.

Tabulka 8: Přehled investic do navrhnutých protiopatření

navrhnuté protiopatření	cena řešení (bez DPH)
stavební úprava serverovny, klimatizace	42 000
zálohování pomocí LTO2 pásek	70 200
konfigurace Active Directory a Group Policy	8 000
přechod na Windows XP Profi	27 000
zavedení bezpečnostní politiky	35 000
školení uživatelů	15 950

Stavební úpravy budou prováděny údržbáři - zaměstnanci firmy Top Moravia Q, s.r.o. Zálohování, Win XP Professional a konfigurace vychází z průměrných cen náhodně zvolených firem v ČR. Zavedení bezpečnostní politiky a školení uživatelů (v rozsahu 2 hodin) je vypočítáno jako náhrada nákladů na mzdy zaměstnanců.

Následující tabulka obsahuje údaje, o kolik se snížilo riziko jednotlivých hrozeb po zavedení navrhnutých protiopatření.

Tabulka 9: Porovnání rizika před zavedením navrhovaných protiopatření a po jejich zavedení

Hrozba	Četnost výskytu (1 - nejmenší četnost, 5 - největší četnost)	Zranitelnost dat (1 - nejmenší zranitelnost, 5 - největší zranitelnost)						Riziko (1 - nejmenší riziko, 25 - největší riziko)	
		DB ByznysWin		DB Intranet		dokumenty uživatelů			
		před	po	před	po	před	po	před	po
Krádež	1	2	1	2	1	4	2	2,7	1,3
Poškození paměťového média	2	1	1	3	1	5	2	6	2,7
Chyba zaměstnanců	3	2	2	3	2	4	2	9	6
Přístup neautorizovaným uživatelem	1	2	1	1	1	3	1	2	1

3.3.1 Fyzická bezpečnost

Náklady na postavení příčky s uzamykatelnými dveřmi a klimatizací jsou 42.000,- Kč. Tímto opatřením se zajistí přístup k samotným serverům pouze kompetentním osobám. Hodnota dat zde umístěných není vyčíslitelná, škoda vzniklá vyzrazením důvěrných dat se podle majitelů firmy pohybuje řádově v milionech Kč. Vzhledem k hodnotě zabezpečených zařízení a dat je investice zanedbatelná.

3.3.2 Zálohování

Zálohování všech firemních dat na pásky LTO2, včetně SW a konfigurace vyjde na 70.200,- Kč. Souhrnné náklady na obnovu všech dokumentů a databází vytvořených v jeden pracovní den jsou 18.373,- Kč, měsíční potom 367.460,- Kč. Výpočet těchto nákladů vychází z kapitoly 3.1.3.1 *Náklady na obnovu dat.* V této sumě není započítána hodnota zálohovaných e-mailů, které mají pro společnost minimální hodnotu. Pokud by firma potřebovala získat data archivovaná např. před 2 týdny, investice do zálohovacího systému by se vyplatila. V této oblasti je lepší prevence (mít kvalitní zálohování všech dat), než o data nenávratně přijít (popř. mít k dispozici pouze pár záloh). Investici do nového systému zálohování tedy rozhodně doporučuji.

3.3.3 Centrální politika bezpečnosti

Nakonfigurování Active Directory a Group Policy bude firmu stát 8.000,- Kč, připojení počítačů do domény (včetně nákupu MS Windows Professional) vyjde na 27.000,- Kč. Celkem tedy 35.000,- Kč.

Připojení do domény umožní správci snadněji konfigurovat nastavení serverů (zálohování, ISA Server) a jednotlivých uživatelských účtů (oprávnění instalování programů, atd…). Pro některé navrhované změny je zavedení centrální bezpečnostní politiky výchozí, proto je investice do MS Windows Professional nezbytná.

3.3.4 Zavedení bezpečnostní politiky

Náklady na zavedení bezpečnostní politiky a školení uživatelů jsou přibližně 40.000,- Kč. Tyto náklady jsou vypočítány jako náhrada nákladů na mzdy zaměstnanců.

Jelikož zaměstnanci denně pracují s firemním majetkem a daty v hodnotě řádově milionů Kč, je zavedení bezpečnostní politiky zanedbatelným výdajem.

Všechny investice do počítačových technologií a nejmodernějšího zabezpečení je zbytečné, pokud s nimi bude pracovat nezkušený uživatel. Bezpečnostní školení uživatelů je nezbytné pro správné a účinné fungování navržené bezpečnostní politiky.

4 Závěr a doporučení

V mé bakalářské práci jsem se zaměřil na oblast počítačové bezpečnosti firemních dat a bezpečnostní politiky. V první kapitole jsem analyzoval současné zabezpečení informačních technologií a systémů v konkrétní firmě Top Moravia Q, s.r.o. Zjištěný stav informačních technologií nelze označit za kritický, nicméně byla zjištěna celá řada různě závažných nedostatků.

V druhé kapitole popisuji bezpečnostní politiku a základní pojmy počítačové bezpečnosti v prostředí Microsoft Windows.

Úkolem této práce bylo navrhnout řešení nalezených nedostatků. Vzhledem k rozsahu této práce jsem se zaměřil zejména na snížení rizika uskutečnitelnosti hrozeb působících na firemní data. Tento návrh přináším v poslední kapitole, která je rozdělena do dvou celků. První celek obsahuje technická protiopatření, druhý pak bezpečnostní politiku.

V závěru práce hodnotím efektivitu vložených investic nutných k realizaci návrhů. Vzhledem k velikosti firmy a její závislosti na výpočetní technice hodnotím aplikaci navrhovaného řešení za finančně nenáročnou. Pro opravdu bezpečný informační systém je ale potřeba, aby se do systému řízení bezpečnosti aktivně zapojili všichni zaměstnanci a osvojili si základní bezpečnostní návyky.

Ač firma zatím neměla větší problémy, či ztráty v důsledku havárie nebo útoku na IS/IT, je potřeba se tomuto úskalí věnovat a nebrat ho na lehkou váhu. Doufám, že vedení společnosti si uvědomí hrozící nebezpečí a do budoucna přeji firmě co nejméně problémů.

Seznam použité literatury

Knihy

[1] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 2004. ISBN 80-251-0106-1.

[2] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. 2005. ISBN 80-251-0574-1.

[3] ENDORF, C., SCHULTZ, E. a MELLANDER, J. *Hacking – detekce a prevence počítačového útoku*. 2005. ISBN 80-247-1035-8.

[4] HANÁČEK, P. a STAUDEK, J. *Bezpečnost informačních systémů*. 2000. ISBN 80-238-5400-3.

[5] HORÁK, J., KERŠLÁGER, M. *Počítačové sítě pro začínající správce*. 2001. ISBN 80-7226-566-0.

[6] NORTHCUTT, S. *Bezpečnost počítačových sítí*. 2005. ISBN 80-251-0697-7.

[7] PROSISE, CH. a MANDIA, K. *Počítačový útok Detekce, obrana a okamžitá náprava*. 2002. ISBN 80-7226-682-9.

České technické normy

[8] ČSN 36 9786 – ČSN ISO/IEC 13335 1-4 – *Informační technologie – Směrnice pro řízení bezpečnosti IT*.

[9] ČSN 36 9789 – ČSN ISO/IEC 15408 1-3 – *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT*.

[10] ČSN 36 9790 – ČSN ISO/IEC 17799 – *Informační technologie – Soubor postupů pro management bezpečnosti informací.*

Firemní materiály

[11] KAMAN, M. a KOPÁČEK, J. *Předimplementační příprava systému ByznisWin*. 2006. Dokumentace informačního systému.

[12] VANĚČEK, P. *Oběh účetních dokladů*. 2000. Interní směrnice.

[13] VANĚČEK, P. *Organizační řád*. 2000. Interní směrnice.

Časopisy

[14] DOUCEK, P., Bezpečnost IS/ICT a proces globální integrace. *AT&P journal*, 2005, č. 1, s. 65 - 66. ISSN 1335-2237.

[15] DOUCEK, P., Budování systému řízení bezpečnosti IS/ICT. *AT&P journal*, 2005, č. 2, s. 86 - 88. ISSN 1335-2237.

Internetové adresy

[16] *Bezpečnost*. [online] Dostupné z: http://www.root.cz/bezpecnost. Poslední úprava 18.5.2008.

[17] *CA ARCserver Backup*. [online] Dostupné z: http://www.ca.com/us/data-loss-prevention.aspx. Poslední úprava 7.2.2008.

[18] *Microsoft*. [online] Dostupné z: http://www.microsoft.com/cs/cz. Poslední úprava 25.5.2008.

[19] *Top Moravia Q, s.r.o.*. [online] Dostupné z: http://www.topmoravia.com. Poslední úprava 14.3.2008.

Seznam použitých zkratek

DB	Database (databáze)
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
HDSL	High bit-rate Digital Subscriber Line
IS	Information Systems (informační systém)
ISDN	Integrated Services Digital Network (digitální síť integrovaných služeb)
IT	Information Technology (informační technologie)
LAN	Local Area Network (lokální počítačová síť)
MySQL	Structured Query Language
PHP	Hypertext Preprocessor
PPTP	Point-to-Point Tunneling Protocol
RAID	Redundant Array of Independent Disks (vícenásobné pole nezávislých disků)
VPN	Virtual Private Network (virtuální privátní síť)
WAN	Wide Area Network (rozsáhlá počítačová síť)

Seznam obrázků a tabulek

Seznam příloh

Příloha 1: Směrnice o zálohování dat

Top Moravia Q, s.r.o.

Zálohování dat

Interní směrnice č. 10

Obsah:

1. Úvodní ustanovení

Směrnice o zálohování dat je vnitřním normativním předpisem společnosti TOP MORAVIA Q, s.r.o.

Směrnice pro zálohování dat blíže popisuje způsob zálohování, uložení pásek a obnovu dokumentů vytvořených zaměstnanci společnosti při činnosti společnosti.

Ustanovení jsou závazná pro všechny pracovníky společnosti.

Vedoucí pracovníci na všech stupních řízení jsou povinni vhodnou formou seznámit podřízené pracovníky s obsahem Směrnice a dbát na její dodržování. Každý pracovník společnosti má právo nahlédnout do Směrnice, která je uložena u generálního ředitele společnosti.

2. Doba do revize směrnice

Směrnice bude podrobena revizi po dvou letech případně po 5 změnách směrnice.

3. Zálohování dat

3.1 Odpovědná osoba

Odpovědná osoba za zálohování je pan XXX, v jeho nepřítomnosti jej zastupuje p. XXX. Tato odpovědná osoba je povinna provádět výměnu pásek LTO2 v zálohovací mechanice. Tato výměna se provádí každý pracovní den, dle stanoveného schématu.

3.2 Zálohovaná data

- Uživatelské dokumenty (pokud jsou uloženy v adresáři dokumenty synchronizované se serverem), platí pro počítač zavedený v Active Directory
- Informační systém Byznys
- Intranetový informační systém
- Data na sdílených discích
- Nastavení serveru

3.3 Způsob zálohování

Data se zálohují na magnetické pásky LTO2 s kapacitou zálohy 200/400 GB.

Zálohování probíhá každý pracovní den, systémem GFS (denní, týdenní a měsíční zálohy). Zálohování probíhá ve večerních hodinách.

4. Uložení pásek

Veškerá záloha obsažená na magnetických páskách musí být bezpečně uložena mimo serverovnu a mimo dosah jakékoli neodpovědné osoby

Denní záloha dat bude uložena v trezoru společnosti.

Týdenní záloha dat bude uložena na bezpečném místě: XXX

Měsíční záloha dat bude uložena na bezpečném místě: XXX

5. Obnova dat

Na základě požadavku odpovědné osoby provede p. XXX obnovu dat z magnetických pásek. K tomuto úkonu je třeba znát:

- Název dokumentu nebo složku, kterou je třeba obnovit
- Datum potřebné obnovy
- Umístění, kam má být obnova provedena

6. Kontrolní činnost

Pan XXX namátkově provádí kontrolu provedených záloh, takovým způsobem, že provede obnovu dat na předem připravené datové úložiště 1 x měsíčně.

Tato směrnice nabývá účinnosti dne 20.5.2008

Roman Z a v a d i l

jednatel společnosti